Pennsylvania Homeless Management Information System (PA HMIS)

Appendix A: PRIVACY AND SECURITY PLAN

2015

Adopted on: Western CoC PA-601 November 13, 2015
Version: [1.0]

Contents

DEFINITIONS

Covered Homeless Organization (CHO)

Any organization (employees, volunteers, and contractors) that records, uses or processes

Protected Personal Information Protected Personal Information (PPI)

Any information about a homeless client that (1) identifies a specific individual, (2) can be manipulated so that identification is possible, (3) can be linked with other available information to identify a specific individual

ARTICLE 1: PURPOSE

Clients are uniquely identified by a database-managed identity field. For reporting purposes, PA HMIS usually de-duplicates clients at the Program level, per HUD-accepted practice. For purposes of system-wide data sharing and de-duplication, clients with a high enough threshold of quality profile data are identified by a globally unique Master Client ID, which allows system-wide de-duplication. These global IDs are constantly maintained by the system with algorithms that examine client data to determine if matches can be made as data is updated/ added.

ARTICLE 2: ROLES AND RESPONSIBILITIES

HMIS Lead

A rarely used "super user" privilege level used by DCED staff to allow "Manage Agency" access to multiple agencies (a service area). In jurisdictions that have an HMIS lead, certain System Administration duties, such as enforcement of policies and procedures may be assumed by this individual on behalf of the System Administrator.

System Administrator

Full privileges to PA HMIS - PA HMIS System Administrator, Help Desk, and programmers only

CoC HMIS System Administrator / Agency Manager

The Agency Manager is authorized by their agency's Executive Director within the agency having the appropriate authority. The Agency Manager cannot use PA HMIS COLLABORATIVE until after signing a System User Agreement with their agency, and completing the necessary training. This Agency Manager is responsible for following the policies and procedures outlined in this

document, and are ultimately responsible for collecting and entering client data in as real time as possible depending on the project type. The Agency Manager will also act as the point of contact for client data and reporting done within the system.

Agency Managers are responsible for the following:

- Serves as the primary contact between the Authorized Agency and DCED/ PA HMIS.
- Must have a valid email address and be an active, trained user.
- Manages agency user accounts; adding and removing authorized users for their agency; Agency Managers are required to remove users from the PA HMIS immediately upon termination from agency, placement on disciplinary probation, or upon any change in duties not necessitating access to PA HMIS information. All changes must be relayed to the PA HMIS System Administrator or proxy.
- Must be technically proficient with web-based software since he/she will be responsible for maintaining the Authorized Agency's PA HMIS organizational structure and information.
- Has access to all client data, user data, and agency administration information for the Authorized Agency; thus, is responsible for the quality and accuracy of this data.
- Ensures the stability of the agency connection to the Internet and PA HMIS, either directly or in communication with other technical professionals.
- Trains agency end users, if necessary; this includes training all Authorized Agency staff on how to use PA HMIS as well as training to ensure compliance with privacy and security policies.
- Provides support for the generation of agency reports.
- Monitors and enforces compliance with standards of client confidentiality and ethical data collection, entry, and retrieval at the agency level.

Assistant Agency Manager / Case Manager

The Assistant Agency Manager / Case Manager is authorized by their agency's Executive Director within the agency having the appropriate authority. The Assistant Agency Manager / Case Manager cannot use PA HMIS COLLABORATIVE until after signing a System User Agreement with their agency, and completing the necessary training. The Assistant Agency Manager / Case

Manager is responsible for following the policies and procedures outlined in this document, and are ultimately responsible for collecting and entering client data in as real time as possible depending on the project type.

Clients

Clients choose to participate in PA HMIS COLLABORATIVE with written authorization to allow an agency's user to collect and enter their personal information into PA HMIS COLLABORATIVE. It is extremely important in the use of PA HMIS COLLABORATIVE that client confidentiality, privacy, and security are maintained at a very high level. The policies and procedures written in this document fulfill basic HUD HMIS requirements, utilize best practices for the industry, and are further enhanced for the Balance of State CoCs.

ARTICLE 3: SECURITY

For user authentication, PA HMIS maintains the following:

a) User permissions are assigned by role and by Agency/Site
b) Users are logged out of the system after a configurable period of inactivity (15 minutes)
c) Passwords must be changed periodically (90 days)
d) Inactive users can be locked out, if necessary

An audit trail of changes is maintained for all user-editable objects in history tables that track when changes were made, by whom, and the previous value(s).

PA HMIS uses HTTPS/SSL Standards for data transmission.

Password expiration is handled by PA HMIS Helpdesk. The password rules are: Passwords must be at least six (8) characters long and contain at least one upper-case letter, one lower-case letter, one number, and one symbol. Passwords must be updated every 90 days, and cannot be reused.

Baseline Requirements

A CHO must apply system security provisions to all the systems where personal protected information is stored, including, but not limited to, a CHO's networks, desktops, laptops, mini-computers, mainframes and servers.

Security has three categories:

- System Security
- Software Application Security
- Hard Copy Security

Additional Requirements

A CHO may commit itself to additional security protections consistent with HMIS requirements by applying system security provisions to all electronic and hard copy information that is not collected specifically for the HMIS. A CHO may also seek an outside organization to perform an internal security audit and certify system security.

System Security: User Administration

Authorizing Personnel for PA HMIS COLLABORATIVE

Policy: *Only authorized individuals who have successfully completed the requirements for access to the system including training and completion of a System User Agreement may be allowed to access PA HMIS COLLABORATIVE on behalf of an agency.*

PA HMIS System User License Agreement

Policy: *A PA HMIS COLLABORATIVE PA HMIS System User Agreement must be signed and kept on file for all agency personnel or volunteers, past or present that will collect or use PA HMIS COLLABORATIVE data on behalf of the agency. The original signed PA HMIS COLLABORATIVE PA HMIS System User Agreement will be filed at DCED in the agency's PA HMIS COLLABORATIVE file. Additionally, each agency is required to keep a copy of all of their PA HMIS System User Agreements on file at their office location so that DCED may review this documentation during monitoring visits. At No Exceptions should an individual who has not signed a PA HMIS System User Agreement be able to have or gain access to use of a PA HMIS System User License at any time.*

Description:

The PA HMIS System Agreement is a document between a participating agency and its employees, contractors, or volunteers who are authorized to collect PA HMIS COLLABORATIVE data and/or record client data into the system, for the purpose of agreeing to abide by the rules and regulations defined in the HMIS Data and Technical Standards, Final Notice, Federal Register, Volume 69, No. 146 as published on Friday, July 30, 2004.

Designate Agency System User

Policy: *The agency's Executive Director or an Agency designated personnel must designate individuals to act as the agency's System User(s).*

Description:

The System User is accountable for the following items:

- Maintain the agency programs and services profiles in the system;
- Act as the main point of contact for PA HMIS COLLABORATIVE System Administrator (DCED);
- Ensure client privacy, confidentiality, and security;
- Maintain compliance with technical requirements for participation;
- Store and enforce System User Agreements;
- Post Compliance Notice;
- Enforce data collection, entry, and quality standards in a real-time process
- Assist DCED with On-Site Technical Assistance/Audits

Designating PA HMIS COLLABORATIVE PA HMIS System User License

Policy: *Any individual working on behalf of the agency (employee, contractor, and volunteer), that will enter information into PA HMIS COLLABORATIVE database must be designated as a PA HMIS COLLABORATIVE System User; and therefore is subject to these policies and procedures.*

Description:

Anybody who collects any PA HMIS COLLABORATIVE data (electronic or paper) or creates reports from the system must receive training. This training is varied depending on the person's role. If someone will not be entering anything into the system but will be explaining PA HMIS COLLABORATIVE to others, the System Agency Manager is required to train this person on client privacy, confidentiality, and security procedures. Individuals, who will work with the PA HMIS COLLABORATIVE software, will be required to attend the Policies and Procedures training as well as specific training on the PA HMIS COLLABORATIVE software.

Assigning User Workgroup Permissions Level

Policy: *PA HMIS COLLABORATIVE System Administrator will assign users an appropriate User Workgroup Permissions level such that the users only has access to PA HMIS COLLABORATIVE functionality or information required to successfully fulfill their agencies*

roles. The PA HMIS COLLABORATIVE System Administrator will also maintain the agency's Approved Users List. The Executive Director or empowered officer will then contact PA HMIS COLLABORATIVE System Administrator to set-up user Workgroup Permissions Levels in the system and to schedule their designated PA HMIS System User(s) for training. User ids and passwords will not be distributed to new users until after they have completed the required PA HMIS COLLABORATIVE training with the PA HMIS COLLABORATIVE System Administrator.

Description:

Within PA HMIS COLLABORATIVE, each user is assigned a workgroup permission level based on the tabs to which they have access. This security allows the user to gain access to certain areas of the PA HMIS COLLABORATIVE application. This security feature is utilized to ensure that individuals can only access the type of client information they need to do their job within the agency. An example would be that an agency would be assigned two different workgroup permissions. Agency Manager is designated for the entire agency and can view all information for all programs within their agency only. Assistant Manager and/ or Case Manager is designated for the individual program within the agency, therefore would only have access to view information for the individual program within the agency.

User Workgroup Permission Levels

Policy: *All PA HMIS Users will have a level of permission to data that is appropriate to the duties of their position so that information is recorded and accessed on a "need to know" basis. All users should have the level of access that allows efficient job performance without compromising the security of the PA HMIS or the integrity of client information.*

Procedure: Each Agency Manager (and/or its Executive Director) will identify the level of access each licensed user will have to the PA HMIS database. Privilege levels were detailed previously in the roles and responsibilities section.

Removing Authorized Personnel

Policy: *The PA HMIS COLLABORATIVE System Administrator must be notified within 24 hours and in writing by the designated Agency personnel when an individual is no longer authorized to access PA HMIS COLLABORATIVE on the agency's behalf.*

Passwords

Policy: *Users will have access to the PA HMIS via a user name and password. Passwords must be changed a minimum of once every 90 days. Users will keep passwords confidential. Under no circumstances shall a user share a password nor shall they post*

their password in an unsecured location; to do so will be considered a breach of the system user agreement and will trigger appropriate repercussions and/or sanctions for both the user and agency.

Procedure: *Upon sign in with the user name and temporary password, the user will be required by the software to select a unique password that will be known only to him/her. Every 90 days, passwords are reset automatically by the PA HMIS software. User has a maximum of up to seven times to enter the correct login information. After seven(7) times of failed logins the system automatically looks out the user account for security purposes and the password will have to be recovered/ reset.*

Password Recovery

Policy: *PA HMIS staff has access to User accounts, but not unique passwords. Users must contact the PA HMIS Helpdesk for password resets.*

Procedure: In the event of a lost or forgotten password, the user will have to send a PA HMIS Helpdesk ticket to reset their password. Within the helpdesk request the following should me included; username, organization, and that the password needs to be reset. Once users receive an email back from the PA HMIS Helpdesk, which contains a temporary password, Users must login and change their password immediately before PA HMIS will allow them access to Agency and Client data.

DCED Communication with Authorized Agencies

Policy: *The PA HMIS System Administrator or proxy is responsible for relevant and timely communication with each agency regarding the PA HMIS. The PA HMIS System Administrator or proxy will communicate system-wide changes and other relevant information to Agencies as needed. He/she will also maintain a high level of availability to Authorized Agencies.*

Procedure: General communications from the PA HMIS System Administrator will be directed towards all users. Specific communications will be addressed to the person or people involved. The PA HMIS System Administrator will be available via email, phone, and mail. The notification function in PA HMIS and the PA HMIS email list will also be used to distribute HMIS information. While specific problem resolution may take longer, the PA HMIS System Administrator will strive to respond to Authorized Agency questions and issues within 24 hours of receipt. Agency Managers are responsible for distributing information to any additional people at their agency who may need to receive it, including, but not limited to, Executive Directors, client intake workers, and data entry staff. Agency Managers are responsible for communication with all of their agency's users.

Authorized Agency Communications with DCED (non-technical, i.e. Policy and System Administration)

Policy: *Authorized Agencies are responsible for communicating non-technical needs and questions regarding the PA HMIS directly to the PA HMIS System Administrator. In order to foster clarity both for PA HMIS users and for PA HMIS, ALL non-technical communications with DCED regarding the PA HMIS must go through the PA HMIS System Administrator.*

Procedure: Agency Managers at Authorized Agencies will communicate needs above and beyond daily help desk technical assistance needs directly with the PA HMIS System Administrator. Examples of these needs are, but not limited to questions about policies, administration, data requests, and system changes. The PA HMIS System Administrator will attempt to respond to Authorized Agency needs within two business days of the first contact.

Backup procedures, off-site storage facilities and locations where the backup is stored

ClientTrack Hosting & Backup

ClientTrack's data center is a SSAE 16 certified data center. Incremental database backups are performed every 3 hours and full database backups are performed each day and sent offsite weekly to a second geographically disperse SSAE 16 storage facility.

A. Restoration procedures for the application and data at the host level.
B. Recovery procedures for historical data at the host level.
C. A stated recovery time after a planned or unplanned outage, power interruption, or system crash.

ClientTrack Restoration and Recovery

ClientTrack partners with ViaWest, a state of the art managed hosting and colocation datacenter. ViaWest is an SSAE 16 (formerly SAS 70) certified and co-located data center. Data backup and server recovery are covered as part of standard ClientTrack contracts. PA HMIS data is backed up on regular intervals throughout the day and daily backups are maintained for approximately 30 days. Backups are stored on spinning disks so there is limited hardware (old tapes) that need destroyed in accordance with HIPAA guidelines upon decommissioning. Failed drives are properly decommissioned to ensure compliance. Data backup is performed to ensure that hardware and drive failures do not result in the loss of data or system availability. Hosting services include:

- Incremental database backups are performed every 3 hours
- Backups are encrypted with 256-bit AES encryption
- Backups are sent offsite to a secure storage facility weekly

The SaaS hardware/software platform is implemented to be fault tolerant. As an SSAE 16 compliant data center, the data center is designed, tested and certified to withstand and function under disaster conditions without loss of service or data. Additionally, ClientTrack is designed to operate on readily available "commodity" server hardware and standardized Internet connection. In the extremely unlikely catastrophic event, our disaster recovery plans enable the entire ClientTrack SaaS platform to be built from virtual servers in any data center unaffected by the catastrophe.

ClientTrack employs 24x7, a support model to address any needs associated with the server environment. This support is augmented on the ground in two separate geographically disperse locations with ViaWest's expert response teams. ClientTrack has experienced minimal downtime in the last 12 months and proactively works to ensure that remains the company standard.
The first step to resolving a reported problem is to isolate the problem as a network/ hardware problem or connectivity. ClientTrack employs a completely redundant network to allow a failover to occur without disruption to access. This normally rules out a network or hardware issue barring a catastrophic event. As outlined above, clients should immediately contact ClientTrack via the support line if connectivity is disrupted to allow immediate response. ClientTrack will immediately identify and resolve issues associated with access.
In the event of a catastrophic event, ClientTrack employs a series of disaster recovery procedures that are intended to identify possible threats so they can be addressed proactively. This includes a number of troubleshooting steps leading all the way up to activating the disaster recovery site to provide continuity of service. A catastrophic failure resulting in loss of connectivity will be recovered at the disaster recovery site within 4 hours. This allows the recovery network and data propagation to occur across all production environments in the second SSAE 16 facility.
ClientTrack reports any outage events including the cause, resolution, and mitigation steps employed to protect against a future outage. ClientTrack is designed to operate on readily available server hardware and standardized internet connections; in the extremely unlikely catastrophic event, the entire ClientTrack SaaS platform can be restored at a backup data center unaffected by the catastrophe.

Monitored Use

PA HMIS Lead Agency may monitor Participating Agencies and any Authorized User's use of the Service and the Database, and Provider may freely use and disclose any information and materials received from any Authorized User or collected through Participating Agencies and Authorized User's use of the Service, including the Database and Content.

General

Participating Agency records shall be subject to audits, from time to time, that are consistent with the HUD regulations applicable to HMIS. It is the responsibility of the Participating Agency to present any applicable documents to the PA HMIS Lead Agency. At any time during normal business hours and as often as the PA HMIS Lead Agency, HUD, and/or any other government agency entitled to the Content of the Database may require and deem necessary, the Participating Agency shall make available all such records and documents as requested by said parties for audit and/or monitoring. The Provider, HUD, and/or applicable government agencies may examine and make excerpts or transcripts from such records and may audit all contracts, procurement records, invoices, materials, personnel records, etc. relating to all matters covered by this Agreement.

HUD Performance Reviews and Monitoring

The Participating Agency understands that HUD may conduct performance reviews and monitoring of the PA HMIS implementation and of the Participating Agency in order to examine reported statistics, commitment rates, and compliance with eligibility, income targeting, and any other applicable requirements. The Participating Agency agrees to cooperate with HUD and the PA HMIS Lead Agency to undertake such remedial action as may be required pursuant to the HUD Regulations.

Monitoring by the PA HMIS Lead Agency

The PA HMIS Lead Agency may perform periodic monitoring of the Database and Participating Agency's use and entry of information into the same. The Participating Agency agrees to cooperate with the PA HMIS Lead Agency throughout any monitoring procedure and to implement such corrective action as requested.

In the event Monitoring is Not Performed

In the event that any monitoring or performance reviews are not conducted by the PA HMIS Lead Agency, HUD, and/or any other government agency, the Participating Agency shall not be excused from obligations to abide by all terms of this Agreement, all rules of PA HMIS Governance Charter and any HMIS or applicable HUD regulations.

ARTICLE 3: PA HMIS PRIVACY

The Participating Agencies shall at all times comply with the HMIS Program Regulations in addition to all of the aforestated regulations, codes, statutes, laws, associated Executive Orders, OMB Circulars, other applicable Federal regulations, and all future revisions and amendments to the same. The Participating Agencies shall become thoroughly familiar with all of the foregoing requirements as applicable and shall ensure that the use of the Services complies in all respects.

A. The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and all rules and regulations promulgated pursuant to the authority granted therein, including but not limited to, those set forth in 45 C.R.F. §§ 160-164 (2003), all as supplemented, replaced and amended from time to time.

B. Federal confidentiality regulations as contained in the Code of Federal Regulations, 42 C.F.R. Part 2 regarding disclosure of alcohol and/or drug abuse records. In general terms, the federal rules prohibit the disclosure of alcohol and/or drug abuse records unless disclosure is expressly permitted by written consent of the person to whom it pertains or as otherwise permitted by CFT Part 2. A general authorization for the release of medical or other information is not sufficient for this purpose.

C. Pursuant to the HUD Data and Technical Standards Final Notice published in the Federal Register on March 29, 2010 and the PA-HMIS Governance Charter, each Participating Agency will prominently display a PA-HMIS Notice of Privacy Practices or a notice developed by the Participating Agencies that incorporates the content of the Continuum approved PA-HMIS Notice of Privacy Practices form, in its program offices where intake occurs, and will provide written copy of the Notices to all Clients enrolling in the Participating Agencies programs and services. The Subscriber will update its Notice of Privacy Practices as needed to comply with federal law and regulations and with the PA-HMIS policy changes.

No Unauthorized Access

Participating Agencies shall not permit unauthorized access to the Service or any of the Content. Neither Participating Agencies nor any of its Sub-Contractors shall permit their clients, customers, vendors, consultants, service providers, agents, contractors, subcontractors, business partners, consortium partners, joint venture partners, affiliates (other than wholly owned subsidiary), concessionaires, subscribers, members, or associative/cooperative members or employees thereof access to the Service, Content, or any portion of the Database or Information, other than as may be expressly permitted herein. The Participating Agency shall immediately notify PA HMIS Administrator upon learning of any unauthorized access, or the actual or potential compromise or breach of any security measures related to the Service or Content.

Personal Information

Medical or personal information of individuals may be in the Database, or otherwise contained or entered into the Content ("Personal Information"). Some or all of the Personal Information

may be subject to the Health Insurance Portability and Accountability Act ("HIPAA") of 1996, or other state or federal laws providing protection and safe guards for relevant Personal Information ("Privacy Laws"). Subscriber shall ensure that it is familiar with any applicable Privacy Laws, and shall be responsible for ensuring that no violation of those Privacy Laws occurs through Participating Agency's use of the Service. PA HMIS Lead Agency shall take reasonable actions and endeavor to comply with all Privacy Laws, but the PA HMIS Lead Agency is not responsible for the breach of any Privacy Laws by the Participating Agency, or any other participating agency and the information that they may add to the Content and Database. Upon being notified of any violation or potential violation of Privacy Laws, The PA HMIS Lead Agency will take such reasonable actions as it deems necessary and fit to remain compliant with the Privacy Laws.

Inter-Agency Data Sharing

Policy: *PA HMIS is an "open" system, meaning that data can be shared between PA HMIS participating agencies. Whether data is actually shared or not is determined on a per client basis, based on user input and client data sharing preferences.*

If the client elects to have their information shared partially or completely, and the agency with the initial service begins working with another agency not participating in PA HMIS, then those agencies must use the Inter-Agency Partnership Data Sharing Agreement.

Explanation: The need for client confidentiality and the benefit of integrated case management needs be balanced. During the initial PA HMIS planning process (conducted in 2006), providers and DCED were not in favor of electronic data sharing within PA HMIS. However, in light of new regulations and community needs, this position has been reversed. PA HMIS has been redesigned to permit Inter-Agency data sharing while still safeguarding client confidentiality.

Procedure: When new clients are entered into PA HMIS, the initiating user must set the Client's data sharing permission (called a data sharing policy, based on the Client's response on the Release of Information form) before data sharing is permitted. These permissions control the information that is shared about the client globally. If no data sharing policy is set up, PA HMIS assumes that data sharing is not permitted. Additionally, users must complete a Domestic Violence Assessment before the client record can be created. This assessment is capable of overriding data sharing options. If a client is recorded as fleeing a domestic violence situation, not only is data sharing locked down, but only that user and Agency Managers will be able to view that client's record.
Users must record the actual responses received by the client when setting up the client's electronic data sharing policy. Users may be monitored to ensure compliance with this policy at any time by Agency Managers, HMIS Leads, or the PA HMIS System Administrator, in which case users will need to provide a copy of any Release of Information forms that are requested. Any user found to not adhere to the data sharing permissions allowed by the client will be immediately and permanently banned from PA HMIS, and may face possible legal action. If a user feels it is in the best interest of the client, they may further restrict the information that is shared by disallowing extra data elements in the client's electronic

sharing policy, but users may never choose to implement a less restrictive data sharing policy without collecting a new Release of Information form that has been signed by the client and permits less restrictive data sharing.

Ethical Data Use

Policy: *Data contained in the PA HMIS will only be used to support or report on the delivery of homeless and housing services in Pennsylvania. Each PA HMIS User will affirm the principles of ethical data use and client confidentiality contained in the PA HMIS Policies and Standard Operating Procedures Manual, the PA HMIS Participation Agreement, and the PA HMIS System User Agreement. Each Authorized Agency must have a written privacy policy, including specific policies related to employee misconduct or violation of client confidentiality. All PA HMIS Users must understand their Agency's privacy policy, and a signed policy statement must become a permanent part of the employee's personnel file.*

Procedure: All PA HMIS users will sign a PA HMIS System User Agreement before being given access to the PA HMIS. Any individual or Authorized Agency misusing, or attempting to misuse PA HMIS data will be denied access to the database, and his/her/its relationship with DCED or the PA HMIS may be terminated. Any Authorized Agency for which the relationship with DCED or PA HMIS is terminated will also likely be de-funded by DCED and/ or the Continuum of Care in which they are located because of the statutory requirement to participate in the Continuum's HMIS.

Access to Core Database

Policy: *No one but DCED/ PA HMIS staff will have direct access to the PA HMIS database through any means other than the PA HMIS user interface, unless explicitly given permission by DCED during a process of software upgrade, conversion, or for technical assistance.*

Procedure: Client Track, DCED's IT department, and PA HMIS staff will monitor both our web application server and our database server and employ updated security methods to prevent unauthorized database access.

Client Rights and Confidentiality of Records

Policy: *PA HMIS operates under a protocol of inferred consent to include client data in the PA HMIS. Each Authorized Agency is required to post a sign about their privacy policy in a place where clients may easily view it (i.e. - at the point of intake, on a clipboard for outreach providers, in a case management office). The privacy posting should include a statement about the uses and disclosures of client data as outlined in this document. Written authorization for inclusion of a client's data in PA HMIS is not required, but is inferred when a client accepts the services offered by the program and when the privacy posting is displayed for client review.*

Clients may opt out of PA HMIS or be unable to provide basic personal information. Clients have the right of refusal to provide personal identifying information to the PA HMIS, except in cases where such information is required to determine program eligibility or is required by the program's funders. Such refusal or inability to produce the information shall not be a reason to deny eligibility or services to a client. When a client exercises his/her right of refusal, de-identified demographic (anonymous) information will be entered into the PA HMIS.

Each Authorized Agency shall take appropriate steps to ensure that authorized users only gain access to confidential information on a "need-to-know" basis in accordance with this document and their own Privacy Policy. Duly authorized representatives of DCED may inspect client records (including electronic records) at any time, although non-PA HMIS staff will not, as a matter of routine, be permitted to access protected private information. DCED and Authorized Agencies will ensure the confidentiality of all client data as described in this document.

Explanation: The data in the PA HMIS is personal data, collected from people in a vulnerable situation. DCED and Authorized Agencies are ethically and legally responsible to protect the confidentiality of this information. The PA HMIS will be a confidential and secure environment protecting the collection and use of client data.

Procedure: Access to client data will be controlled using security technology and restrictive access policies. Each Authorized Agency must develop and make available a privacy policy related to client data captured in PA HMIS and through other means. A posting that summarizes the privacy policy must be placed in an area easily viewed by clients, and must also be placed on the Authorized Agency's web site (if they have one). Only individuals authorized to view or edit individual client data in accordance with the stated privacy policies and these Standard Operating Procedures will have access to that data. The PA HMIS will employ a variety of technical and procedural methods to ensure that only authorized individuals have access to individual client data.

Authorized Agency Grievances

Policy: *Authorized Agencies will contact the PA HMIS System Administrator to resolve PA HMIS problems including but not limited to operation or policy issues. If an issue needs to be escalated, the PA HMIS System Administrator may contact DCED's Legal Department. DCED, through the PA HMIS System Administrator, will have final decision-making authority over all grievances that arise pertaining to the use, administration, and operation of the PA HMIS.*

Procedure: Users at Authorized Agencies will bring PA HMIS problems or concerns to the attention of their Agency Manger. If problems, concerns, or grievances cannot be addressed by the Agency Manager, the Agency Manager will contact the PA HMIS System Administrator, who may ask for these issues to be stated in writing. If it is not appropriate to raise the issue with the Agency Manager, users may contact the PA HMIS System Administrator directly via phone, email, or mail. If the grievance requires further attention, the PA HMIS System Administrator may consult with DCED's legal Department. DCED,

through the PA HMIS System Administrator, shall have final decision-making authority in all matters regarding the PA HMIS.

Client Grievances

Policy: *Clients must contact the Authorized Agency with which they have a grievance for resolution of PA HMIS problems. Authorized Agencies will report all PA HMIS-related client grievances to DCED. If the Authorized Agency's grievance process has been followed without resolution, the Authorized Agency may escalate the grievance to DCED as outlined in the "Authorized Agency Grievances" section. At any time, clients may request that their personally-identifying information be removed from the PA HMIS.*

Procedure: Each Authorized Agency is responsible for answering questions, complaints, and issues from their own clients regarding the PA HMIS. Authorized Agencies will provide a copy of their privacy policy and/or copies of the PA HMIS Privacy Policy or PA HMIS Policies and Standard Operating Procedures upon client request. Client complaints should be handled in accordance with the Authorized Agency's internal grievance procedure, and then escalated to DCED in writing if no resolution is reached. DCED is responsible for the overall use of the PA HMIS, and will respond if users or Authorized Agencies fail to follow the terms of the PA HMIS agency agreements, breach client confidentiality, or misuse client data. Authorized Agencies are obligated to report all PA HMIS-related client problems and complaints to the PA HMIS System Administrator, who will determine the need for further action. Resulting actions might include further investigation of incidents, clarification or review of policies, or sanctioning of users and Agencies if users or Agencies are found to have violated standards set forth in PA HMIS Participation Agreements or the Policies and Standard Operating Procedures Manual. Upon the client's request for data removal from the PA HMIS, the Agency Manager will delete all personal identifiers of client data within 72 hours. A record of these transactions will be kept for a period of three years by the Agency Manager and provided to DCED upon request.

Authorized Agency Hardware/Software Requirements

Policy: *Authorized Agencies will provide their own computer and method of connecting to the Internet, and thus to the PA HMIS.*

Procedure: Contact the PA HMIS System Administrator for the current status of assistance.

Hardware/Software Requirements: PA HMIS is web-enabled software; all that is required to use the database is a computer, a valid username and password, and the ability to connect to the Internet using internet browser software (Google Chrome, Firefox, etc.). There is no unusual hardware or additional PA HMIS-related software or software installation required. DCED recommends the following workstation specifications.

Minimum Workstation Requirements

- Computer: PC 500 MHz or better
- Web Browser: Microsoft Internet Explorer 5 or higher, Mozilla Firefox 3.0 or higher, Google Chrome 4.0.249 or higher, or Netscape Navigator 6.0 or higher
- Hard Drive: 2 GB
- 64 MB RAM
- Internet Connectivity (broadband or high-speed)
- SVGA monitor with 800 x 600+ resolutions
- Keyboard and Mouse

Recommended Workstation Requirements

- Computer: 1 Gigahertz Pentium Processor PC
- Browser: Google Chrome v.41 or higher, Mozilla Firefox 29.0 or higher, Internet Explorer 11 or higher, or Safari 5.1.10
- 20 GB Hard Drive
- 512 MB RAM
- Broadband Internet Connection - 128 Kbps (hosted version) or LAN connection
- SVGA monitor with 800x600 + resolution
- Keyboard and mouse

Although there is no unusual hardware or additional PA HMIS-related software required to connect to the database, the speed and quality of the Internet connection and the speed of the hardware and could have a profound effect on the ease of data entry and report extraction. DCED also recommends the use of Windows 7 or higher (1 GHz models or faster) as the Windows platform to eliminate certain technical problems and a high-speed Internet connection.

ARTICLE 4: Appendices

- PA HMIS Privacy Policy (Master)
- PA HMIS Privacy Posting